How To | Configure Microsoft® Windows XP** Virtual Private Network (VPN) client interoperability with NAT-T support

Introduction

This document describes how to provide secure remote access through IP security (IPSec) Virtual Private Networks (VPNs). The solution allows for IPsec NAT Traversal, which is an enhancement to IPsec and ISAKMP protocols that lets VPN clients communicate through Network Address Translation (NAT) gateways over the Internet.

For example, business travellers commonly use IPsec on their laptop to gain remote VPN access to the central office. When working off-site, these users sometimes need to connect to the Internet through a NAT gateway such as from a hotel. NAT gateways are often part of a company's firewall and let its Local Area Network (LAN) appear as one IP address to the world. For more information about NAT gateways, refer to RFC 1631*"The IP Network Address Translator (NAT)"*, and to the *Network Address Translation* section in the Internet Protocol chapter of your device's Reference Manual.

This VPN solution is suitable for any business deployment and provides your office with secure Internet access and firewall protection, plus remote encrypted VPN access for your travelling staff. The solution may be combined with an office-to-office VPN solution with NAT-Traversal (NAT-T) support if required. NAT-T is designed to solve the problems inherent in using IPSec with NAT.

Please refer to the *Configuration Examples* section in your device's Reference Manual, release 2.6.4 or later.

What information will you find in this document?

This document is divided in to the following sections:

- Typical network scenario, on page 2
- Solution requirements, on page 3
- Hardware and software versions used during the setup, on page 5
- Security advice, on page 6
- Loading the NAT-T update to Windows XP, on page 7
- Configuring the VPN client, on page 8
- Configuring the AR450S or other ATI VPN router, on page 15
- VPN Testing, Verification and Troubleshooting, on page 20

Typical network scenario

Consider the following typical network scenario:

You are the manager of a small business and you have purchased the AR450S for your small office premises. You have five PCs networked together with a server in your office. You intend to use your AR450S as your Internet gateway and for it to provide firewall protection.

You also have a team of five sales people who travel widely around the globe. You would like these staff members to have secure (encrypted) remote access through the Internet to the servers in your office—allowing them to access files, private Intranet and business email.

The travelling staff members will get secure remote access from any hotel or location with Internet access through the use of IPSec VPN. Each staff member has a laptop or other portable device with Windows XP or Windows 2000 installed.

This document describes how to configure the Windows system to use IPSec VPN to connect your travelling staff laptops to your AR450S router. Through the use of NAT-T technology, your IPsec VPN will still work even if the remote location or your small office uses a NATing gateway or firewall for Internet access.

When your travelling staff want to connect to the office they simply use the VPN icon on their desktop to initiate the IPSec VPN connection.

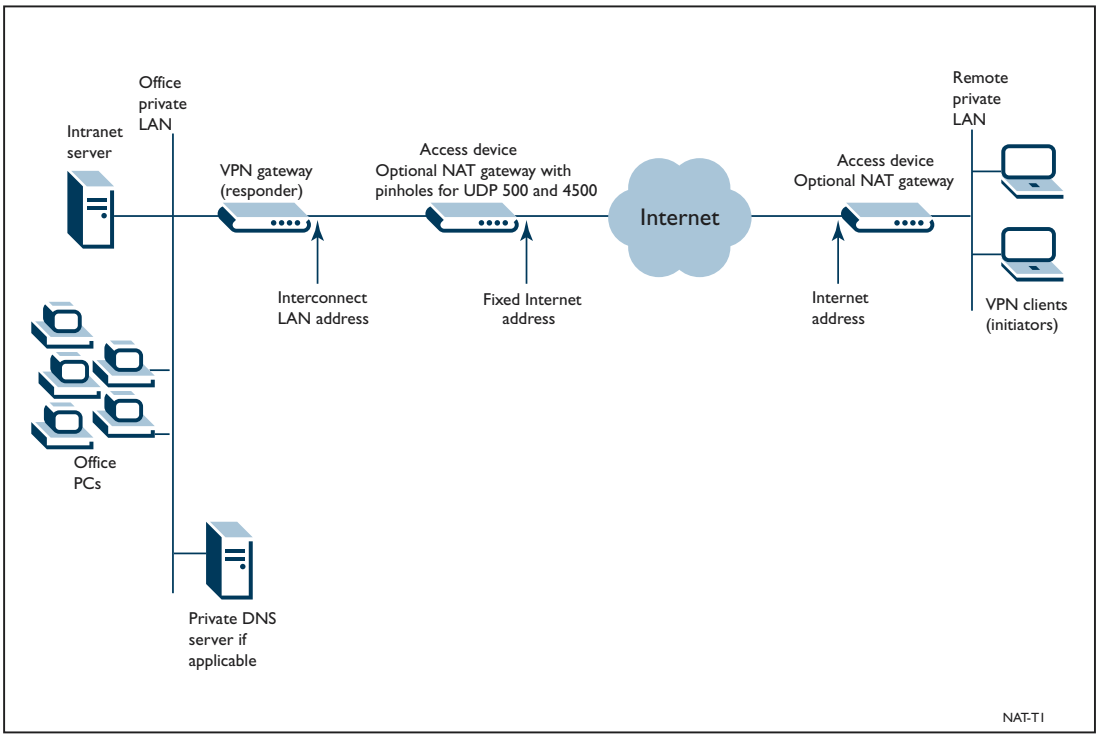


Figure 1: Typical network scenario

Solution requirements

NAT-T is available from software release 2.6.4 or 2.6.6 for the following products:

- AR410
- AR450s
- AR44xx series routers
- AR700 series routers

Other products may include NAT-T with future software releases.

The following products depend on either the Encryption Mini Accelerator Card (EMAC) or the Encryption PCI Accelerator Card (EPAC) to perform encryption.

- The AR300 series router family
- The AR410 router
- The AR700 series router family
- The Rapier series switches.

While the switching products can be configured as VPN gateways, this is usually not a recommended practice. Doing so means you will lose wire-speed switching of data, because all traffic needs to be inspected by the Firewall and IPSec modules at CPU processing speed.

On all products, feature licences are required if you want to access Triple-Digital Encryption Standard (3DES) or Advanced Encryption Standard (AES) encryption. Single DES is available by default on purchase of the encryption card. 3DES and AES are strategic export encryption products and you will need to apply to your local Allied Telesyn Office or Distributor before purchasing the feature licences.

An ISAKMP licence should already be loaded on your router. If not, contact your local distributor.

Note: *An encryption card is not necessary on the AR450S or AR44x series, as it is built into the product.*

If you wish to configure a Microsoft Windows 2000 VPN call with NAT-T support, refer to the *"How To Configure Microsoft Windows 2000 Virtual Private Network (VPN) Client Interoperability with NAT-T support"* document at http://www.alliedtelesyn.co.uk/en-gb/solutions/techdocs.asp

For the VPN client solution given in this document to work, your office must have a fixed Internet address. This is the target address for the VPN client. Depending on whether the office uses a NATing gateway device or not, this Internet address will either belong to the NAT gateway or the VPN peer router (see Figure 1).

Please note that many ISPs assign dynamic addresses as standard practice, and these addresses can change periodically. It is likely you will need to specifically ask for a fixed address for your office.

If the office uses a NATing gateway device, it must be configured with allow rules (or "pinholes") for UDP 500 and UDP 4500 traffic.

Other solution requirements and things to consider

- Other utilities sometimes conflict with the Windows IPSec policy agent, and may need uninstalling—such as another VPN Client installation, or perhaps a firewall utility. In some cases the uninstall of these utilities may not properly restore the Windows IPSec policy agent, in which case you may need to check your Windows services listing to see that the agent is in 'automatic' mode.
- If your office VPN router is behind an external gateway that does not use NAT—perhaps a firewall or IP filtering device—then the external gateway will need a protocol 50 permit rule in addition to the UDP 500 and UDP 4500 permit rules. This will allow NAT-T to work in all situations.
- Your ISAKMP pre-shared key needs to be alphanumeric only, not hexadecimal, to ensure interoperation with Windows.
- Users will need to define a PPP DNS server address on the router that will be assigned to the incoming VPN users. The DNS address needs to be valid for the network being connected to via VPN.
- Internet Explorer browser users may need to define a proxy definition against the VPN dial up link, valid for the network being connected to via VPN.
- If you have the customised "ProhibitIPSec" registry entry or a customised MMC IP Security Policy defined in Windows—you should remove these and reboot, i.e. from a previous attempt to use Windows IPSec client.
- Using Secure Shell for remote management is encouraged. Telnet should not be used to a secure gateway.

Hardware and software versions used during the setup

The following hardware and software was used to prepare the configuration example in this document:

- The AR450S (or you could use any of the other products mentioned above).
- Software release 2.6.4 or 2.6.6.
- Appropriate 3DES and/or AES licence for the Allied Telesyn Layer 3 products.
- PC running Microsoft Windows XP Professional or Home Edition, Service Pack 1a.
- KB 818043 patch, or Windows XP Service Pack 2, loaded onto Microsoft Windows. See the following section for details.
- If you have Windows XP Service Pack 2 (and you want NAT-T to support NAT at the responder VPN gateway end of the link), you will need to refer to instructions at KB885407 on the Microsoft support site. Please note that you will make a registry key entry, and this key can be set for different values depending on your NATing circumstances. More detail is available in later sections.

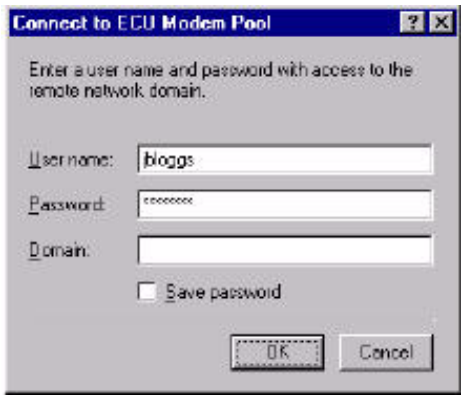
Security advice

Since this Windows VPN solution is usually used to allow remote access from portable PCs and laptops into corporate networks, a common security concern is "What happens if my remote laptop or PC is stolen or falls into unauthorised hands?"

Take some extra precautions to make portable PCs and laptops more secure.

Users are advised to:

- Avoid using computer bags, as they advertise the fact that you have a PC.
- Never leave access numbers or passwords in your carrying case.
- Carry your laptop with you.
- Encrypt your data.
- Buy a laptop security device, e.g. a security cable to securely attach it to a heavy chair, table, or desk.
- **Not** use the **Save Password** feature that Windows offers during dial-up. I.e. do not tick the box labelled "Save password" in the dialog box shown below.



Some PCs have security modes that can be enabled, for example Toshiba's HDD password utility. There are also numerous tips to be found relating to laptop security, available on the Web.

Loading the NAT-T update to Windows XP

To ensure that your version of Windows XP operating system supports NAT-T you will need to fulfil one of these pre-requisites:

- The recommended method is to ensure Windows XP Service Pack 2 has been installed. To get a copy of the service pack go to:
  http://www.microsoft.com/athome/security/protect/windowsxp/choose.mspx
- If you do not have the service pack installed, you will need to install the update patch for Knowledge Base article KB 818043.

Either way, the details of this NAT-T enhancement can be read at:
http://support.microsoft.com/?kbid=818043.
This update includes improvements to IPSec to better support virtual private network (VPN) clients that are behind network address translation (NAT) devices.

The list of fixes included in Windows XP SP2 is at the following URL:
http://support.microsoft.com/default.aspx?scid=kb;en-us;811113

The release notes for Windows XP SP2 are at the following URL:
http://support.microsoft.com/default.aspx?scid=kb;en-us;835935

Note: *If either of these requirements are not met, then on connection attempt the router or switch log will not proceed beyond "ISAKMP MAIN Phase 1 (resp) started with peer x.x.x.x" and "Exch xx: Failed". If you have ISAKMP debugging enabled, this condition will show as "Remote ID different to expected".*

After installing the update and rebooting your computer, you can configure the Windows XP VPN client. See the following sections.

Support for NAT device at the responder VPN gateway end of link

As mentioned in the earlier section, Windows XP SP2 does not support NAT devices at the VPN responder end of the link. To overcome this issue, you need to refer to instructions on the Microsoft support site in Knowledge Base article 885407:

http://support.microsoft.com/default.aspx?kbid=885407

This article describes a change required in the Windows registry. It also outlines some security issues with this solution.

Please note that you will make a registry key entry, and this key can be set for different values depending on your NATing circumstances:

- value 0 (default): does not permit IPSec when responders are behind NAT.
- value 1: XP SP2 can initiate IPSec to responders behind NAT (you will target the public side of the NAT device and that device will need pinholes).
- value 2: XP SP2 can initiate IPSec when both initiator and responder and behind NAT.

For more detail, please refer to the KB article.

Configuring the VPN client

Creating a VPN tunnel from the PC host to the Allied Telesyn VPN gateway router.

1. On your desktop, click ***Start*** > ***Control Panel***

Make sure you are in *Category View*, as shown in Figure 2. If your computer is in Classic View, click **Switch to Category View** in the Control Panel Menu on the left of your screen.

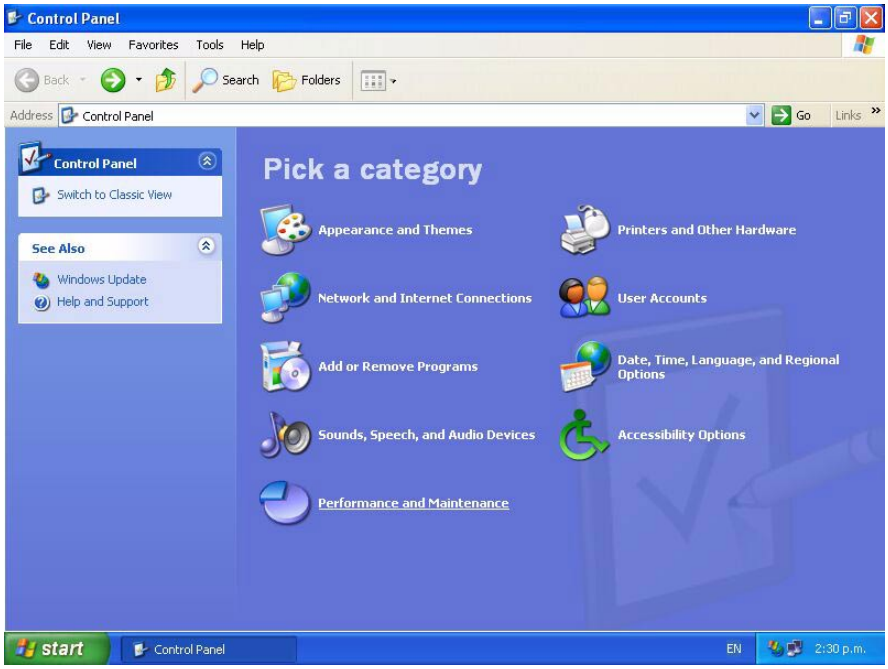


Figure 2: Example output showing Category View

2. Click ***Network and Internet Connections*** > ***Create a connection to the network at your work place***

This starts up the New Connection Wizard.

3. Select ***Virtual Private Network Connection*** as shown in Figure 3.

Figure 3: Example output showing connection creation options

4. Click **Next**.

5. Type in a name for the connection (e.g. VPN Connection To Head Office) as shown in Figure 4.

Figure 4: Example output showing connection name.

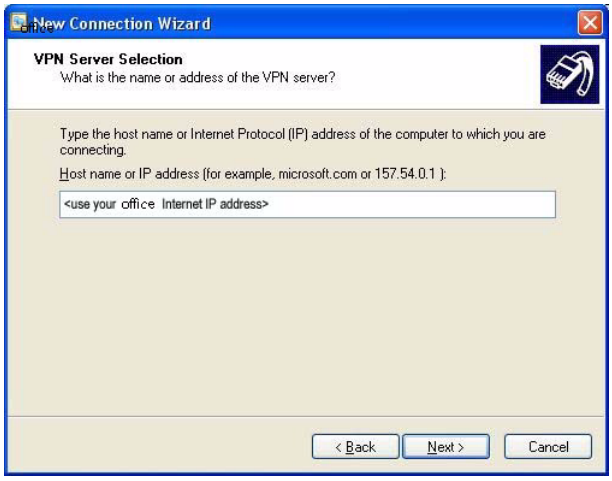
6. Click **Next**.

If you have a modem installed, you will see the screen shown in Figure 5a. Here you may assign an associated dialled call or select *Do not dial the initial connection*. If you choose the latter, you will need to manually connect the modem or have LAN access available before initiating this VPN call. **Go to Step 7.**

If you do not have a modem installed you will see Figure 5b. Go to Step 8.

Figure 5a: with modem installed

Figure 5b: without modem installed



7. If you have a modem installed, and you see Figure 5a, select *Do not dial the initial connection,* and click **Next**.
8. Enter the name or IP address of your office Internet address. This should be a fixed Internet address, either configured on your NAT gateway if you have one, or on your router or switch. In the case of the NAT gateway, pinholes or allow rules will be needed (refer to the diagram on page 2).
9. Click **Next**.

You have now completed creating the connection as shown in Figure 6.

10. Check the *Add a shortcut to this connection to my desktop* checkbox

Figure 6: Example output from the final window of the New Connection Wizard.

11. Click **Finish**.

12. **Close or Minimise** the *Network and Internet Connections* window.

Connect to the Head Office

Note: *The pre-shared key used in this procedure (Step 9) needs to be the same ISAKMP pre-shared key as defined on your Allied Telesyn router in the ENCO definitions. Refer to AR450S Configuration, on page 15. The pre-shared key needs to be alphanumeric to ensure interoperation with Windows.*

1. Double-click the new *Head Office* icon on your desktop.
2. Enter your **user name** and **password** as shown in Figure 7

Note: *Your user name and password will be the same as is configured on your router user database or RADIUS server.*

Figure 7: Example output showing connecting to Head Office

3. Click in the *Save this user name and password for the following users*.
4. Select *Me only*. This is recommend for enhanced security.
5. Click **Properties**.

This opens the *Head Office Properties* window as shown in Figure 8.

6. Click the **Security Tab**.

Figure 8: Example output showing the Head Office Properties Security Tab

7. Click the **IPSec Settings** button.

This opens the *IPSec Settings* window as shown in Figure 9.

Figure 9: Example output showing the IPSec Settings window.

8. Click in the *Use pre-shared key for authentication* check box.
9. Enter your **pre-shared key**.
   The pre-shared key needs to be the same ISAKMP pre-shared key as defined on your Allied Telesyn router in the ENCO definitions. Refer to "AR450S Configuration" on page -15. Note that the pre-shared key needs to be **alphanumeric** to ensure interoperation with Windows.
10. Click **OK**.

You are now back to the *Head Office Properties* window.

11. Click the **Networking Tab**

Figure 10: Example output showing Head Office Properties Networking Ta

12. In the *Type of VPN* drop-down box, select *L2TP IPSec VPN*.

13. Click **OK**.

You have now completed configuring the L2TP client.

14. Click **Connect**.

Note: *The connection will fail if the router has not been configured.*

Configuring the AR450S or other ATI VPN router

This configuration is a script file for running IPSec encapsulating L2TP, on a Head Office AR450S configured to support IPSec remote PC clients. You could also use any other ATI VPN router.

Before loading the configuration, you will need to: create a security user, enable system security, log in as the security user and then create a general ENCO key for use with ISAKMP—all done from the command line prompt. These steps are outlined below. Then you may load the script using ZMODEM or TFTP methods, or use the router's built in editor or command-line prompt.

1. **Define a security officer.**

   This step must be completed on the head office router.

   ```
   add user=secoff password=<your password> privilege=securityofficer
   enable system security
   login secoff
   ```

2. **Generate a key at the head office router.**

   ```
   create enco key=1 type=general
      value=<enter your own alphanumeric string>
   ```

   Note the value of the string you have entered so that you can load it on the PC clients. This shared key will be used to encrypt initial ISAKMP negotiation. The shared key must be alphanumeric to ensure interoperation with Windows. If you also want to use Secure Shell, you will need additional keys. Refer to the Secure Shell chapter and example in your device's software reference for more information.

3. **Enter the configuration.**

AR450S Configuration

The following commands need to be loaded as a file using zmodem or FTTP; or they can be entered at the command line and saved using the command:

```
create conf=vpn.cfg
```

After you have created the file, set your router configuration to refer to this configuration at boot time using the command:

```
set conf=vpn.cfg
```

The configuration starts here and ends on page 19

Note: *To understand the generic address names below, please refer to the diagram on page 2. Comments are indicated in the script below using the # symbol.*

```
# An optional help file is available: http://www.alliedtelesyn.co.nz/support/
  updates/help.html

set help=450-261a.hlp

set system name="IPSec Gateway"


# The command below shows the Security Officer inactive timeout delay. The
  default is 60 seconds. During setup you may decide to use 600 seconds.

set user securedelay=600

add user=secoff pass=<your password> privilege=securityOfficer login=yes

set user=secoff description="Security Officer Account"

del user=manager


# The incoming L2TP calls will be CHAP authenticated. They may be authenticated
  against the router's user database as configured below, or against a RADIUS
  Server if configured. You also have the option of assigning individual
  addresses to individual users using the router user database or your Radius
  server. IP addresses defined in the user database take precedence over the IP
  pool addresses.

add user=dialin1 password=friend1 login=no ip=192.168.8.50

add user=dialin2 password=friend2 login=no

add user=dialin3 password=friend3 login=no ip=192.168.8.51

add user=dialin4 password=friend4 login=no


# If RADIUS server support is needed, use a line such as this:

# add radius server=<your RADIUS server address> secret=<your secret key>


# All dynamic incoming L2TP calls will associate with this PPP template as
  indicated below.

create ppp template=1 bap=off ippool="myippool" authentication=chap echo=30
   lqr=off

# PPP may need to give out the site's private DNS server address so the client
  can do dns lookups

set ppp dnsprimary=<your private DNS server address, if applicable>
```

```
# To cater for dynamic creation of incoming L2TP calls enter the following
  commands.
enable l2tp
enable l2tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1
enable ip
add ip int=vlan1 ip=<office private LAN address>
add ip int=eth0 ip=<interconnect LAN address> mask=<appropriate mask>

# The default route to the Internet..
add ip route=0.0.0.0 mask=0.0.0.0 int=eth0 next=<your NAT gateway or ISP next-
   hop address>

# The IP pool addresses are the internal address ranges you want to allocate to
  your IPSec remote PC clients (e.g. ip=192.168.8.1-192.168.8.254). Although,
  addresses defined in the user database will take precedence.
create ip pool=myippool ip=x.x.x.x-x.x.x.x

# Firewall
enable fire
create fire policy=main
create fire policy=main dy=dynamic
add fire policy=main dy=dynamic user=ANY
add fire policy=main int=vlan1 type=private

# Dynamic private interfaces are accepted from L2TP, which are from IPSec only.
add fire policy=main int=dyn-dynamic type=private
add fire policy=main int=eth0 type=public

# The firewall allows for internally generated access to the Internet through
  this NAT definition.
add fire policy=main nat=enhanced int=vlan1 gblinterface=eth0

# This NAT definition allows Internet access for remote VPN users by providing
  address translation.
add fire policy=main nat=enhanced int=dyn-dynamic gblinterface=eth0

# Rules 1 and 2 allow for ISAKMP and the "port floated" IKE /ISAKMP that NAT-T
   uses.
add fire policy=main rule=1 int=eth0 action=allow protocol=udp ip=<office
   Internet address> port=500 gblip=<office Internet address> gblport=500
add fire policy=main rule=2 int=eth0 action=allow protocol=udp ip=<office
   Internet address> port=4500 gblip=<office Internet address> gblport=4500
```

```
# Rule 3 becomes the L2TP tunnel allow rule. Additional security is provided by
  only allowing traffic from IPSec tunnels.

add fire policy=main rule=3 int=eth0 action=allow prot=udp ip=<office Internet
    address> port=1701 gblip=<office Internet address> gblport=1701 encap=ipsec


# Using Secure Shell for remote management is encouraged. Telnet should not be
  used to a secure gateway. You need to define appropriate RSA enco keys. See
  the Secure Shell chapter and example in your software reference for more
  information.

enable ssh server serverkey=2 hostkey=3 expirytime=12 logintimeout=60

add ssh user=secoff password=<secoff password> ipaddress=<trusted remote ip
    address>


# IPSEC configuration

create ipsec saspecification=1 key=isakmp protocol=esp encalg=3desouter
    hashalg=sha mode=transport

create ipsec saspecification=2 key=isakmp protocol=esp encalg=3desouter
    hashalg=md5 mode=transport

create ipsec saspecification=3 key=isakmp protocol=esp encalg=des hashalg=sha
    mode=transport

create ipsec sas=4 key=isakmp protocol=esp encalg=des hashalg=md5
    mode=transport


# The ORDER of proposals is important. You should propose the strongest
  encryption first.

create ipsec bundle=1 key=isakmp string="1 or 2 or 3 or 4"


# The first two IPSec permit rules allow for IKE /ISAKMP and the "port floated"
  IKE plus NAT-T traffic port.

create ipsec policy="isakmp" int=eth0 ac=permit

set ipsec policy="isakmp" lp=500

create ipsec policy="isakmp_float" int=eth0 action=permit

set ipsec policy="isakmp_float" lport=4500


# This is a generic IPSec policy. Using the peer=any options allows multiple
  IPSec remote PC clients to connect through this same policy.

create ipsec policy="all_roaming" int=eth0 action=ipsec key=isakmp
  bundlespecification=1 isakmppolicy="roaming1" peer=any

set ipsec policy="all_roaming" transport=udp lport=1701


# If you need both VPN and internet-browsing access, use the following internet
  policy. Do not use this policy for VPN only.

create ipsec policy="internet" int=eth0 action=permit

enable ipsec
```

```
# If the "internet" permit policy is used, then the "isakmp" and "isakmp_float"
  permit policies are actually optional.


# ISAKMP Configurations*
create isakmp policy="roaming1" peer=any key=1
set isakmp policy="roaming1" senddeletes=true localid=local natt=on
enable isakmp


# You may find these alias commands (shortcuts) handy if debugging analysis is
  needed
add alias=ed string="enable isa debug"
add alias=ed2 string="enable ipsec poli debug=all"
add alias=dd string="dis isa debug"
add alias=dd2 string="dis ipsec poli debug=all"


*# If you are running release 273-02 or later, you will notice that NAT-T is now
  off by default (CR6652). YOu will need to turn it on:
 set isakmp policy=”roaming1” nattraverasal=on
# The default was changed to support customers with legacy configurations using
  the proprietary IPSEC udptunnel mode.
```

Don’t forget to create and save the config.

```
create conf=vpn.cfg
set conf=vpn.cfg
```

This is the end of the configuration

Support Limits

In making design decisions for your IPSec VPN network, please be aware that your actual tunnel throughput and the number of tunnels you can support is affected by your Internet connection speed at both the VPN Client and the VPN router, and also by Internet congestion. Available throughput on any one tunnel is also affected by the current loading on other active VPN tunnels.

Figures on maximum VPN throughput for Allied Telesyn’s range of VPN products are often available through your Allied Telesyn distributor or reseller.

VPN Testing, Verification and Troubleshooting

If your VPN tunnel is not successful, the following troubleshooting notes will help establish the cause of the problem.

If needed, you may contact your Allied Telesyn distributor or reseller, or your local Allied Telesyn support desk for assistance.

Testing an IPSec tunnel on your router

This first section looks at troubleshooting your router.

Before starting the verification commands below, recheck your router configuration using the command **sh conf dyn**.

The "IP local" IP address is best left at default. If "IP local" is set to an address other default, this may invalidate ISAKMP negotiation. Use the command:

```
set ip local ip=0.0.0.0
```

It is good practice to confirm that traffic is being encrypted. A good initial check is to observe the ISAKMP negotiation entries in the system log using the command `sh log`. There will be several phases of negotiation, and they should indicate successful completion. If you can see no negotiation entries in the log, or if you only see an initial start and no completed phases, then this suggests a configuration error, or no ISAKMP negotiation received from the peer. Checking, with the command **sh fire event**, will allow you to see what traffic has been received from the peer, and if it has been allowed by the firewall. You may also confirm ISAKMP and IPSec progress with the **sh isakmp sa** and **sh ipsec sa** commands, plus the **sh isakmp exchange** command.

Confirmation that traffic is actually being encrypted is best seen by using a counter command such as **sh ipsec poli=to_hq count**. Every time you ping a set of 4 pings, the "outProcessDone" counters (in the Outbound Packet Processing Counters section) should increment by 4. Also, the echo reply traffic should cause the "inProcessDone" counters (in the Inbound Packet Processing Counters section) to increment by 4.

It is important that the IPSec policies are configured in the correct order.

If you have a "permit" IPSec policy with open policy address selectors, (intended to allow unencrypted Internet access), then this policy must be configured last – after the **action=ipsec policies** command. Otherwise this permit policy will process all traffic and no traffic will be encrypted. The order of the IPSec policies can be checked by the **sh ipsec poli** command. In the output of this command, each policy is assigned a position number.

Troubleshooting an IPSec tunnel

If problems continue, then ISAKMP and IPSec debugging modes may be used. Turning on all debug modes is rather verbose, so we recommend basic ISAKMP debugging initially. Capture the following debugging:

```
ena isakmp debug=state
```

- You can also use the command:

```
ena isakmp debug=trace
```

- Attempt connection from your IPSec remote PC client
- To end your debugging trace use the command:

```
dis isakmp debug=all
```

If the basic ISAKMP debugging modes does not reveal a problem to you, then all debugging modes should be enabled and captured to a text file and sent to your support centre. Use the commands

- ena ipsec poli=tunnel debug=all
- `ena isakmp debug`

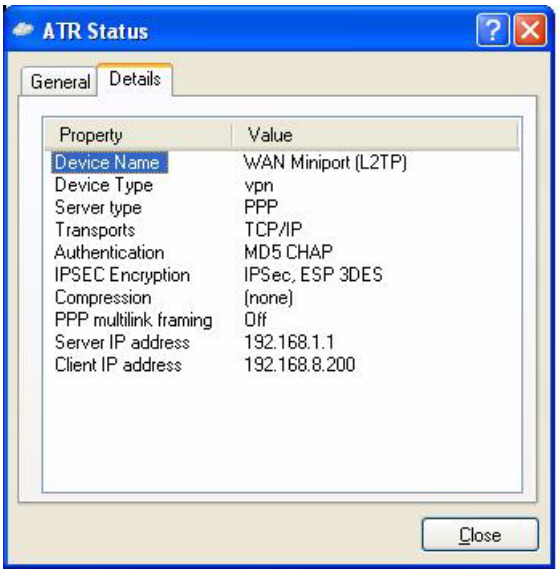
Also capture **`sh log`** to show ISAKMP log entries (as mentioned above), **capture sh fire event** and **sh debug**. Forward all this debugging to your local technical support for analysis. Your local support centre also have access to advanced support centres if necessary. Allied Telesyn offers technical assistance in partnership with our authorised distributors and resellers. For technical assistance, please contact the authorised distributor or reseller in your area. Please refer to *http://www.alliedtelesyn.com* for a list of Allied Telesyn's authorised distributors & resellers.

Testing an IPSec tunnel on your PC

If you wish to check your connection, right-click your connection icon (e.g. Virtual Private Connection to Head Office) in the Network Connections folder, or on your desktop.

This will display the window shown in Figure 11.

Figure 11: Example output from the VPN Connection to Head Office Status window.



1. Click **Status**.
2. Click the *Details Tab* to check your connection information.
3. Click **Close**.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesyn.com

C613-16034-00 REV D

Connecting The IP World

Allied Telesyn®